



Aalborg Universitet

AALBORG UNIVERSITY  
DENMARK

## On the minimum distance of one-point geometric Goppa codes

Andersen, Henning Ejnar; Geil, Hans Olav

*Published in:*  
Conference AGCT-10

*Publication date:*  
2005

*Document Version*  
Publisher's PDF, also known as Version of record

[Link to publication from Aalborg University](#)

*Citation for published version (APA):*  
Andersen, H. E., & Geil, H. O. (2005). On the minimum distance of one-point geometric Goppa codes. In F. Rodier, & S. Vladut (Eds.), *Conference AGCT-10: Arithmétique et Théorie de L'Information CIRM*.

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

### Take down policy

If you believe that this document breaches copyright please contact us at [vbn@aub.aau.dk](mailto:vbn@aub.aau.dk) providing details, and we will remove access to the work immediately and investigate your claim.

# On the minimum distance of one-point geometric Goppa codes

Henning E. Andersen and Olav Geil

The Feng-Rao bound gives a lower bound on the minimum distance of codes defined by means of their parity check matrices. From this bound it is clear how to improve a large family of codes by leaving out certain rows in their parity check matrices. In our work we derive a simple bound on the minimum distance of codes defined by means of their generator matrices. From our bound it is clear how to improve a large family of codes by adding certain rows to their generator matrices. Actually our result not only deals with the minimum distance but gives lower bounds on any generalized Hamming weight. Our bound is easily interpreted into the setting of order domain theory. In particular it deals with one-point geometric Goppa codes.

In the remaining part of this extended abstract we consider only one-point geometric Goppa codes. Let  $F/\mathbb{F}_q$  be an algebraic function field with a single place  $P_\infty$  at infinity. Let  $P_1, \dots, P_n$  be rational places,  $P_i \neq P_\infty$ ,  $i = 1, \dots, n$ . Consider

$$\begin{aligned} D &:= P_1 + \dots + P_n \\ R &:= \cup_{m=0}^{\infty} (\mathcal{L}(mP_\infty)) \\ ev_D : \begin{cases} R & \rightarrow \mathbb{F}_q^n \\ x & \mapsto (x(P_1), \dots, x(P_n)) \end{cases} \end{aligned}$$

Let  $W = \{m_1, m_2, \dots\}$ ,  $0 = m_1 < m_2 < \dots$ , be the set of pole numbers of  $P_\infty$ . Choose a basis  $\mathcal{B} = \{f_1, f_2, \dots\}$  for  $R$  as a vector space over  $\mathbb{F}_q$  such that  $\nu_{P_\infty}(f_i) = -m_i$ ,  $i = 1, 2, \dots$ . Consider the one point geometric Goppa code

$$C_{\mathcal{L}}(D, m_j P_\infty) := \text{span}_{\mathbb{F}_q} \{ev_D(f_i) \mid i = 1, \dots, j\}.$$

Let  $1 =: i_1 < i_2 < \dots < i_n$  be such that

$$C_{\mathcal{L}}(D, m_{i_s} P_\infty) \neq C_{\mathcal{L}}(D, m_{i_{s-1}} P_\infty)$$

for  $s = 2, \dots, n$ . Define

$$S := \{m_{i_1}, m_{i_2}, \dots, m_{i_n}\} \subseteq W.$$

Consider any subset  $T \subseteq S$  and the corresponding code

$$E(T) := \text{span}_{\mathbb{F}_q} \{ev_D(f_{i_s}) \mid m_{i_s} \in T\}.$$

Note, that if  $T$  is chosen as the smallest  $k$  elements in  $S$  then  $E(T)$  is a one point geometric Goppa code. Define

$$\sigma : \begin{cases} S & \rightarrow \mathbb{N} \\ m_{i_s} & \mapsto \#\{m_{i_t} \in S \mid \exists m_{i_v} \in S \text{ such that } m_{i_s} + m_{i_v} = m_{i_t}\} \end{cases}$$

### PROPOSITION

$$d(E(T)) \geq \min\{\sigma(m_{i_s}) \mid m_{i_s} \in T\}.$$

### COROLLARY

$$\begin{aligned} d(C_{\mathcal{L}}(D, mP_{\infty})) &\geq \min\{\sigma(m_{i_s}) \mid m_{i_s} \in S, m_{i_s} \leq m\} \\ &\geq n - \deg(mP_{\infty}) = n - m \end{aligned}$$

The proof of the proposition simply relies on the following observation. Let  $*$  be the componentwise multiplication. Then if

$$\vec{c} * \vec{b}_1, \dots, \vec{c} * \vec{b}_{\sigma}$$

are linearly independent we must have  $w_H(\vec{c}) \geq \sigma$ .

### References

- [1] H. E. Andersen, O. Geil, The Missing Evaluation Codes from Order Domain Theory, (June 2004), submitted.